UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,646	03/16/2004	Harlan Seymour	20423-08590	3936

34415 7590 09/17/2008

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
LEWIS, ALICIA M	

ART UNIT	PAPER NUMBER
2164	

NOTIFICATION DATE	DELIVERY MODE
09/17/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	Application No.	Applicant(s)	
	10/802,646	SEYMOUR ET AL.	
	Examiner	Art Unit	
	Alicia M. Lewis	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-11,14,15,17-20 and 23-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-11,14,15,17-20 and 23-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is responsive to the communication filed June 9, 2008. Claims 1, 5, 6, 8, 9, 14, 15, 17, 18, 24, and 26 are currently amended. Claims 1-6, 8-11, 14, 15, 17-20 and 23-26 remain pending in this application.

Claim Objections

1. Claims 1-4 and 23 are objected to because of the following informalities: Claim 1 should be amended to start with the word "An" (i.e. An apparatus), and claims 2-4 and 23 should be amended to start with the word "The" (i.e. The apparatus) to show proper dependence on claim 1. Appropriate correction is required.

2. Claims 1-4 and 23 are objected to because the claimed invention is directed to non-statutory subject matter. Claims 1-4 and 23 recite a plurality of modules configured to perform specific tasks. However, according the specification, page 6 lines 26-27, the modules may be implemented in software. Therefore, claims 1-4 and 23 are directed to software, per se, and are objected to as being non-statutory. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1).

With respect to claim 1, Mattson teaches an apparatus for empirically adjusting access to a database, said apparatus comprising:

coupled to the database, a database discovery module configured to determine database structure and the user's authorized access to the database (paragraphs 32 and 34-36), the user's authorized access including a set of authorized database tables and authorized columns (paragraph 38);

coupled to the database, a command monitoring module configured to monitor the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns (paragraphs 33 and 50) (*A preselected quantity can be any number of accesses, including just one access. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson*); and

coupled to the database discovery module and to the command monitoring module, an analysis module configured to compare the user's actual accesses with the user's authorized accesses and configured to adjust the user's authorized accesses

taking into account results of the comparing by changing settings within a database access control module (paragraphs 37-39, 42-46 and 52).

Although Mattson teaches adjusting a user's authorized accesses to an authorized database table or an authorized column (paragraphs 38 and 46), he does not explicitly teach adjusting the user's authorization to deny future access to authorized tables/columns that were previously authorized, but not accessed.

Ludwig teaches a modular business transactions platform (see abstract), in which he teaches denying future access to authorized tables/columns that were previously authorized, but not accessed (paragraph 51) (*Ludwig teaches disabling a user's access after a certain number of days of nonuse. By disabling a user's access to the system, the user will be denied access to previously authorized database tables/columns, such as those handled by a host user in paragraph 44*).

It would have been obvious to a person having ordinary skill in that art at the time the invention was made to have modified Mattson by the teaching of Ludwig because denying future access to authorized tables/columns that were previously authorized, but not accessed would enable Mattson's intrusion detection system to be used in processing financial transactions and would provide more security measures to prevent intrusion, thus providing more functionality (Ludwig, paragraph 51).

With respect to claim 2, Mattson as modified teaches the apparatus of claim 1 further comprising, coupled to the database discovery module and to the analysis

module, a storage area configured to accumulate data generated by the command monitoring module (Mattson, paragraph 33).

With respect to claim 3, Mattson as modified teaches the apparatus of claim 1 wherein the command monitoring module is a sniffer (Mattson, paragraph 5).

With respect to claims 5 and 14, Mattson teaches:

discovering the user's authorized access to the database (paragraphs 32 and 34-36), the user's authorized access including a set of authorized database tables and authorized columns (paragraph 38);

observing the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns (paragraphs 33 and 50) (*A preselected quantity can be any number of accesses, including just one access. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson)*;

comparing the user's actual accesses with the user's authorized access (paragraphs 37 and 42); and

adjusting the user's authorized database access taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server (paragraphs 37-39, 42-46 and 52).

Although Mattson teaches adjusting a user's authorized accesses to an authorized database table or an authorized column (paragraphs 38 and 46), he does not explicitly teach adjusting the user's authorization to deny future access to authorized tables/columns that were previously authorized, but not accessed.

Ludwig teaches a modular business transactions platform (see abstract), in which he teaches denying future access to authorized tables/columns that were previously authorized, but not accessed (paragraph 51) (*Ludwig teaches disabling a user's access after a certain number of days of nonuse. By disabling a user's access to the system, the user will be denied access to previously authorized database tables/columns, such as those handled by a host user in paragraph 44*).

It would have been obvious to a person having ordinary skill in that art at the time the invention was made to have modified Mattson by the teaching of Ludwig because denying future access to authorized tables/columns that were previously authorized, but not accessed would enable Mattson's intrusion detection system to be used in processing financial transactions and would provide more security measures to prevent intrusion, thus providing more functionality (Ludwig, paragraph 51).

With respect to claims 8 and 17, Mattson as modified teaches wherein the discovering step uncovers any:

tables of the database (Mattson, paragraphs 32 and 38);

columns of the database (Mattson, paragraph 32 and 38);

views of the database (Mattson, paragraph 32);

stored procedures of the database Mattson, (paragraph 53);

user-defined functions of the database (Mattson, paragraph 53); and

triggers of the database (Mattson, paragraph 53).

With respect to claims 9 and 18, Mattson as modified teaches wherein the adjusting step comprises at least one of:

suggesting revised database access control settings to a database administrator;

automatically hardening the database for all times of day (Mattson, paragraph 48);

automatically hardening the database selectively based on time of day;

alerting a database administrator (Mattson, paragraphs 43, 44 and 46); and

continuing to monitor the user's accesses to the database after conclusion of the observing step.

With respect to claims 11 and 20, Mattson as modified teaches wherein the database is automatically hardened using database specific application programming interfaces (Mattson, paragraphs 46 and 48).

With respect to claim 23, Mattson as modified teaches wherein the preselected quantity of actual accesses is sufficiently large that all expected functionalities of applications accessing the database are exercised (Mattson, paragraphs 28-29, 33 and 50) *(The only expected functionalities of applications appears to be users using clients*

to access information in the database. Therefore, any preselected quantity of access to the database by clients, is large enough that the expected functionality is exercised).

With respect to claim 24, Mattson as modified teaches storing data generated by the observing of the user's actual accesses to the database in a storage area (Mattson, paragraph 33).

With respect to claim 25, Mattson as modified teaches generating a map of which tables and columns of the database were accessed during the observing (Mattson, paragraphs 32 and 33).

With respect to claim 26, Mattson as modified teaches:

monitoring the user's actual accesses to the database during an extended period occurring after the preselected quantity of actual accessed have been observed (Mattson, paragraphs 35, 42 and 43) *(According to one embodiment, a preselected quantity may be the item access rate. When this is the case, an extended period may be considered any accesses that occur after the item access rate has been reached, as in paragraph 43);* and

generating an alert in real time regarding the user's actual accesses that are observed during the extended period that were not observed within the preselected quantity of the user's actual accesses (Mattson, paragraph 43) *(All accesses observed after the item access rate has been reached, are considered to be observed during the*

extended period, and not observed within the preselected quantity of accesses. When this is the case, as indicated in paragraph 43, an alert is generated.)

5. Claim 4, 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1), as applied to claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 above, and further in view of Low et al. ("DIDAFIT: Detecting Intrusions in Databases through Fingerprinting Transactions") ('Low').

With respect to claim 4, Mattson as modified teaches claim 1.

Mattson as modified does not teach wherein the database is a relational database accessed by a structured query language.

Low teaches a method for using fingerprints to detect illegitimate accesses to databases (see abstract) in which he teaches wherein the database is a relational database accessed by a structured query language (abstract).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Mattson by the teaching of Low because wherein the database is a relational database accessed by a structured query language would enable a fingerprinting process to be used to detect anomalous database accesses involving SQL statements (Low, column 1, page 122).

With respect to claims 10 and 19, Mattson as modified teaches wherein the database is automatically hardened using standard SQL commands (Low, abstract, page 126, column 1; Mattson, paragraphs 46 and 48).

6. Claims 6 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1), as applied to claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 above, and further in view Vaitzblit et al. (US Patent Application Publication 2005/0097149 A1) (Vaitzblit').

With respect to claims 6 and 15, Mattson as modified teaches claims 5 and 14.

Mattson as modified does not teach further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database.

Vaitzblit teaches a data audit system (see abstract), in which he teaches further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database (paragraphs 11 and 48-51).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Mattson by the teaching of Vaitzblit because teach further comprising the step of generating at least one third party report based upon observing actual accesses to the database would enable an efficient data

audit system that would help organizations address data privacy and security issues (Vaitzblit, paragraph 7), and to additionally detect anomalies (Vaitzblit, paragraph 19).

Response to Arguments

7. Applicant's arguments filed June 9, 2008 have been fully considered but they are not persuasive. Applicant argues that Mattson does not teach adjusting authorized access as claimed. Examiner disagrees. Mattson teaches that a user has authorized access to specific database tables and/or columns (paragraph 38). Mattson also teaches (paragraphs 42-46) that a user's access is monitored, compared with authorized access, and analyzed to determine if intrusion is detected. He further teaches "altering the user authorization" (paragraph 46) as a result of the comparing. Thus it is clear that Mattson teaches adjusting authorized access to database tables and columns.

8. Although Applicant further argues that Mattson does not teach adjusting the user's authorization to deny future access to authorized tables/columns that were previously authorized, but not accessed, the Examiner would like to point out that Mattson was not used to teach this limitation. As stated above, Mattson in view of Ludwig was used to teach denying future access to authorized tables/columns that were previously authorized, but not accessed.

9. Lastly, Applicant argues that Ludwig is not related to adjusting user access to databases, and thus does not teach denying future access to authorized tables/columns that were previously authorized, but not accessed. Examiner disagrees. Ludwig

teaches the establishment of accounts, such as for host users, which may be used to handle database administration (paragraph 44). He further teaches disabling a user's account after a certain number of days of nonuse. By disabling a user's account, the user will be denied the previous access he/she had, including access to previously authorized database tables/columns used to handle database administration. It is clear that Mattson teaches adjusting database access to authorized table and columns; thus the combination of Mattson with Ludwig, which teaches denying future access that was authorized but not used, teaches the limitation of adjusting the user's authorized access by changing settings within a database access control module to deny future database access to an authorized database table or column that is not in the set of accessed tables and columns.

10. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alicia M. Lewis whose telephone number is 571-272-5599. The examiner can normally be reached on Monday - Friday, 9 - 6:30, alternate Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on 571-272-4085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Alicia M Lewis/
Examiner, Art Unit 2164
September 4, 2008

/Charles Rones/
Supervisory Patent Examiner, Art Unit 2164